OMAHA

222 South 15th Street, Suite 1005

Omaha, Nebraska 68102

402.344.8020

DES MOINES

801 Grand Avenue, Suite 150

Des Moines, Iowa 50309

515.244.9800

KANSAS CITY

1000 Walnut, Suite 200

Kansas City, Missouri 64106

816.878.6435

This was completed using LimeWire version 4.14.10 basic (free version) released on 09/19/07. This was completed on multiple machines all running Windows XP with SP2. All findings were later verified for accuracy.

Below is a link to a video created which shows the entire process, from search and preview, to a completed download:

http://www.focussolutions.com/downloads/LimeWire.zip

Below is a link to a file called "searches.zip" which is password protected with the password "iknow." This file contains screenshots of actual LimeWire searches that contain inappropriate text. This shows that CP appears on the first page in every example. Notice that the search terms are not CP specific:

http://www.focussolutions.com/downloads/searches.zip

Directories of Importance:

** C:\Documents and Settings\User Name\Incomplete\

This folder will exist for each profile using LimeWire. Files that are actively downloading and files that were canceled before finished downloading are stored here. Files that are canceled will remain in this folder until one of the following occurs:

A)
   1) The file is "Resumed" with LimeWire and allowed to finish downloading where it will be moved to the "Shared" folder.
   2) The file is deleted manually with Windows Explorer.
   3) The file is deleted from the "Library" tab under the "Incomplete Files" section in LimeWire.

The *creation* date of a file will be when the download was started and the *last modified* date will be when the last bit of data was downloaded. The amount of time between the *creation* and *last modified* dates will indicate the amount of time before one of the following occurred:

B)
   1) The file was canceled with LimeWire which stops further downloading.
   2) All remote users sharing the file stopped sharing which will prevent further downloading until the file is shared again.
   3) The suspect's computer was powered down, LimeWire was closed or connection issues prevented further downloading.

While a file is downloading it will resemble the name of the downloaded file with a unique beginning created by LimeWire which resembles "T1234567-". If the file is a video and "Preview Download" is selected within LimeWire a separate file is created named "Preview-T1234567-Name of file.avi". Once LimeWire is completely closed the preview file will be automatically deleted. The amount of time between the creation date of the preview file and the last modified date of the downloading file will be the time between when the video was viewed and one of the three in section B occurred.

The files "downloads.dat" and "downloads.bak" which are further explained in the "Files of Importance" section are found in this directory.

** C:\Documents and Settings\User Name\Shared\

This folder will exist for each profile using LimeWire. Once a file is completely downloaded it is MOVED into this folder from the "Incomplete" folder and the "T1234567-" portion of the name is removed. Note that the "Incomplete" and "Shared" folders are NOT created with the install of LimeWire but when the program is first opened and the user completes the wizard. This wizard will present the ability to change the default location of these folders. Note that when LimeWire is uninstalled both the "Incomplete" and "Shared" folders including all files contained are NOT removed.

** C:\Documents and Settings\User Name\Application Data\LimeWire\

This is the location for all user settings which is further explained in the "Files of Importance" section.

** C:\Program Files\LimeWire

This is where the LimeWire program files are located. None of these files appeared to be altered when a search was performed or when files were downloaded. If LimeWire is opened when uninstalled this directory along with LimeWire.exe and other supporting files will remain. If LimeWire is completely closed when uninstalled all files including this directory are removed.

Application Closed Date and Time:

Each time LimeWire is closed (which will minimize the application so it appears only by the clock) the files listed below will be written with the current date and time this occurred. This is stored in actual text written on each file. The date is not written when LimeWire is opened but only when closed or completely closed.

** installation.props (has extra settings)
** limewire.props (see "limewire.props")
** mojito.props
** questions.props
** tables.props (has extra settings)

When LimeWire is completely closed (no longer by the clock) the modification dates in the files listed below change, along with the files listed above, which will be written with the date and time this occurred. This will pinpoint the date and time that LimeWire was last completely closed verses when it was closed but remained visible by the clock.

** gnutella.net
** spam.dat (if created)

Files of importance:

** limewire.props

This file contains all of the LimeWire settings found under "Tools" –
"Options". Since LimeWire does not use the registry, all settings are
stored in the .props files. All settings including the "Incomplete" and
"Shared" folder locations are found in this file.

** spam.dat

This OFTEN gets confused as the goldmine of search results – this file
is not that. When you install and USE LimeWire this file is not created
until you right click on a file or group of files and select "Mark as
Junk". I did a search for "Burger King" right clicked on the 17 files
found and selected "Mark as Junk". The spam.dat was created and that
file had 181 lines of text. When viewed it was UGLY. There were lots of
hits for "Burger" and "King" but rarely together. When I selected all
the files and selected "Mark as Not Junk" the file went to 103 lines
but still contained lots of hits for both words. This file does not
change when searching or downloading files with LimeWire.

** library.dat

This file changes OFTEN when LimeWire is open and displays the
individual files and folders that are shared and not-shared which is
different than the generic list of shared folders found in
limewire.props. This file is a serialized Java object which will
require a program that understands parsing Java objects to view.

** fileurns.cache

This file displays the files downloaded and located in the "Shared"
folder. If the files are moved or deleted from this folder, it will be
updated to reflect the change in the file next time LimeWire is opened.
This file will have a *last modified* date of the last file downloaded
or, in the case of a deleted or moved file, the last time LimeWire was
opened.

** downloads.dat
** downloads.bak

When LimeWire is uninstalled and later reinstalled the old
"downloads.dat" and "downloads.bak" files along with any incomplete
downloads are used with the new install. When a search is initiated and
a file begins downloading, the old "downloads.bak" is deleted, the old
"downloads.dat" is renamed to "downloads.bak" and a new "downloads.dat"
is created. This reoccurs every time a file begins downloading and when
a file completely downloads.

Below is an example of how a search is recorded inside the "downloads.dat" and "downloads.bak" files:

The text "halo" was used in the search with "Video" as the selected search type. All other parts of the file were removed to reveal only the desired text seen below:

ð sq~6   xxsq~"?@ w   q~ sq~2q~4w \xxxsq~"?@ w   t fileSizesr java.lang.Long;‹ä Ì #ß J valuexr java.lang.Number†¬• "à‹ xp&©Ùt sha1Urnq~ t defaultFileNameq~ t saveFilesq~2tBC:\Documents and Settings\Rich Hoffman\Shared\Halo 3 – Believe.mp4w \xt attributessq~"?@ w   t searchInformationMapsq~"?@ w   t titlet halot xmlt…<?xml version="1.0"?><videos xsi:noNamespaceSchemaLocation="http://www.limewire.com/schemas/video.xsd"><video title="halo"/></videos>t typesr java.lang.Integer â ¤÷ ‡8 I valuexq~At mediasr com.limegroup.gnutella.MediaType7 †ia;]•

LimeWire currently has the ability for five "search types" which will be recorded in the "downloads.dat" and "downloads.bak" files along side the search text used in the search. The five "search types" used are listed below:

        Documents
        Audio
        Video
        Images
        Programs

When the "downloads.dat" is renamed to "downloads.bak," each will contain the same information and MD5. The only time the search word used could not be located in the "downloads.dat" and "downloads.bak" files was when a file was canceled or cleared out of the "Downloads" section of LimeWire or when the application was closed. Since the search words stored in these files are cleared when the application is closed, it is our best practice to unplug the machine live and not to use traditional Windows shutdown methods.

Note that when a file is downloading it stays in "downloads.dat" until finished. At that time the "downloads.dat" will be renamed to "downloads.bak" and the new "downloads.dat" will not contain any information on the downloaded file. This happens every time a file has finished downloading and the file is renamed and moved to the shared folder. These files do not change at any other time (e.g. when only searching) – only when a download is started.

Thank You,

Rich Hoffman
Focus Solutions
rhoffman@focussolutions.com
(402) 306-3427